ACHUSETTS INSTITUTE OF TECHNOLOGY

LINCOLN LABORATORY

LEGENDRE SEQUENCES

Neal Zierler

Approved OGS
Oliver G. Selfridge
Leader, Group 34

Group Report 34-71

2 May 1958

The research reported in this document was supported jointly by the Department of the Army, the Department of the Navy, and the Department of the Air Force under Air Force Contract No. AF 19(122)-458.

LEXINGTON MASSACHUSETTS

LEGENDRE SEQUENCES[1]

Neal Zierler[2]

The Fourier transform A of a sequence $a = \{a(0), a(1), \ldots\}$ of complex numbers of period $p > 0$ is defined to be[3]

$$A(n) = \sum_{k=0}^{p-1} a(k)\, \beta^{kn}, \quad n = 0, 1, \ldots \quad \text{where } \beta = e^{\frac{2\pi i}{p}}$$

and the autocorrelation function ϕ of a is by definition

$$\phi(n) = \sum_{k=0}^{p-1} a(k)\, \overline{a(k+n)}, \quad n = 0, \ldots .$$

A and ϕ obviously have period p also and it is well known and easy to see that ϕ and $|A|^2$ are Fourier transforms of each other. It follows easily that a necessary and sufficient condition for either of ϕ and $|A|$ to be flat (that is, to assume a constant value except for values of the argument which are multiples of p) is that the other be flat. Thus, knowing that a sequence has a flat auto-correlation function is equivalent to possessing certain information concerning its Fourier transform; namely, that its absolute value is flat. In certain applications involving sequences with flat autocorrelation (see Lerner [1]), one wishes to have a more detailed knowledge of the corresponding Fourier

---

(1) The research in this document was supported jointly by the Army, Navy, and Air Force under contract with the Massachusetts Institute of Technology.

(2) Staff Member, Lincoln Laboratory, Massachusetts Institute of Technology.

(3) Cf. Loomis [4], especially § 34B, p. 137; a is to be regarded as a function on the additive group of residue classes modulo p.

transform sequences. The purpose of this note is to exhibit a family of sequences with flat autocorrelation which essentially coincide with their Fourier transforms. The sequences in question also satisfy the often encountered practical requirement that they take on only two or three values.

Let p be an odd prime. If there exists m for a given n such that $m^2 \equiv n \pmod p$, n is said to be a quadratic residue mod p. The Legendre sequences $a = a_p$ (cf. Landau [2, Def. 18, p. 37]) of period p are defined as follows:

$$a(n) = \begin{cases} 1 \text{ if } n \text{ is a quadratic residue mod } p \\ -1 \text{ otherwise}, \end{cases}$$

for $n \not\equiv 0 \pmod p$; for the moment we regard a(0) as an arbitrary complex number.

Theorem.

$$A(n) = \begin{cases} a(0) + \lambda_p a(n) & \text{if } n \not\equiv 0 \pmod p, \\ a(0) & \text{if } n \equiv 0 \pmod p \end{cases}$$

$$\text{where } \lambda_p = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

The proof depends on two elementary properties of the Legendre sequence:

i) $\sum_{r=1}^{p-1} a(r) = 0$, [2, Satz 79, p. 37],

ii) if neither n nor m is a multiple of p, $a(nm) = a(n)a(m)$, [2, Satz 81, p. 38]; and on the following celebrated theorem of Gauss:

$$\sum_{r=1}^{p-1} a(r)\,\beta^{r} = \lambda_p, \quad [2, \text{Satz } 212, \text{p.}155].$$

First, $A(0) = \sum_{r=0}^{p-1} a(r) = a(0)$ by i).

Now suppose $n \not\equiv 0 \pmod p$; then if $r \not\equiv 0 \pmod p$,

$a(r) = a(r)\cdot 1 = a(r)\cdot a(n^2) = a(r)\cdot (a(n))^2 = a(rn)\, a(n)$ by ii).

Hence $A(n) = \sum_{r=0}^{p-1} a(r)\,\beta^{rn} = a(0) + \sum_{r=1}^{p-1} a(r)\,\beta^{rn} = a(0) + a(n) \sum_{r=1}^{p-1} a(rn)\,\beta^{rn}$.

Since p is prime and both of the functions $a(k)$ and β^k of k have p as period, $\sum_{r=1}^{p-1} a(rn)\,\beta^{rn}$ is simply a rearrangement of $\sum_{r=1}^{p-1} a(r)\,\beta^{r}$ and the assertion follows from Gauss's theorem.

If $p \equiv 3 \pmod 4$, $|A(n)|^2 = |a(0) + a(n)\, i\sqrt{p}\,|^2$ is independent of $n \not\equiv 0 \pmod p$ if and only if $a(0)$ is real. Similarly, if $p \equiv 1 \pmod 4$, $|A(n)|^2 = |a(0) + a(n)\sqrt{p}\,|$ is flat if and only if $a(0)$ is purely imaginary. This yields the following results.

Corollary 1. The Legendre sequence a_p with $p \equiv 1 \pmod 4$ has flat autocorrelation if and only if $a_p(0)$ is purely imaginary.

Corollary 2. The Legendre sequence a_p with $p \equiv 3 \pmod 4$ has flat autocorrelation if and only if $a_p(0)$ is real.

Corollary 3. If a is a Legendre sequence and $a(0) = 0$ then a has flat autocorrelation.

Remark. The corollaries may be obtained without difficulty from some combinatorial results of Perron [3]. Cf. also the work of Kelly [5] for some interesting related results. A large class of sequences with flat autocorrelation has been examined by the writer in [6].

BIBLIOGRAPHY

1. Lerner, R., "Signals having uniform ambiguity functions", IRE Convention Record, Information Theory Section, March, 1958.

2. Landau, E., "Vorlesungen über Zahlentheorie", Vol. 1, Chelsea, New York, 1950.

3. Perron, O., "Bemerkungen über die Verteilung der Quadratische Reste". Math. Zeit. 56 (1952) 122-130.

4. Loomis, L.H., "Abstract harmonic analysis", Van Nostrand, New York, 1953.

5. Kelly, J.B., "A characteristic property of quadratic residues", Proc. Amer. Math. Soc., 5(1954) 38-46.

6. Zierler, N., "Linear recursive sequences", submitted to the Journal of the Society for Industrial and Applied Math.